

AMENDMENTS TO THE SPECIFICATION

Please replace the paragraph no. [0008] with the following amended paragraph:

Consider a general case where a proof system is composed of a prover P and a verifier V, which interact with one another so that the verifier V verifies the validity of a proof that the prover Phase-P has a witness W. Hereafter, if $R(X, W)=1$ is satisfied, then it is described as $(X, W)._{\epsilon}R$, where X is common input supplied to both the prover P and the verifier V, W is the witness of X, which is known by the prover P (typically secret information), and $R()$ is a function. Assuming that